UNITED STATES DISTRICT COURT

for the

Eastern District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

MediaLab, Inc. Kik subscriber Jacob Green, email greengo8606@gmail.com, username Shytxcpl

Case No. 7:24-mj-1036-RJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Eastern District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252A §§ 2251	Distribution, Receipt, and/or Possession Child Pornography & Sexual exploitation of children; Production of Child Pornography

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Kasey Bratt, FBI
Printed name and title

On this 23 day of February 2024, Special Agent Kasey Bratt appeared before me via reliable electronic means, was placed under oath, and attested to the contents of this application.

Date: February 23 2024

Judge's signature

City and state: Wilmington, North Carolina

Robert B. Jones, Jr. United States Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

IN THE MATTER OF THE SEARCH OF: INFORMATION ASSOCIATED WITH MEDIALAB, INC. KIK ACCOUNT: SHYTXCPL located on the email servers at MediaLab, Inc. Kik 1222 6th Street Santa Monica, California 90401	Case No. 7:24-mj-1036-RJ

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent Kasey Bratt of the Federal Bureau of Investigation (FBI), a Division of the United States Department of Justice located in Washington, D.C., assigned to the FBI Charlotte Division, Greenville Resident Agency, Greenville, North Carolina (NC), make the following statement in support of a request for a search warrant:

INTRODUCTION

1. I have been employed as a Special Agent with the FBI since 2022. I am currently assigned to the Criminal Enterprise Program for the FBI Charlotte Division, and I am responsible for conducting investigations of potential violations of federal criminal laws focused on financial crime, violent crime, organized crime, public corruption, violation of individual civil rights, drug-related crime, and informant matters associated with these investigative areas. During my career as an FBI Special Agent I have received training, investigated numerous violations, seized evidence, and arrested persons for violations of federal criminal laws.

2. In my capacity as a Special Agent of the FBI, your affiant is authorized to investigate violations of laws and to execute warrants issued under the authority of the United States. I have received extensive training to investigate cases related to child pornography and child exploitation and have had the opportunity to observe and review thousands of examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. § 2251 and 2252A, and I am authorized by law to request a search warrant.

3. This Affidavit is submitted in support of an application under Rule 41 of the Federal rules of Criminal Procedure for a search warrant for the locations specifically described in Attachment A of this Affidavit, including information associated with the **KIK user name shytxcpl** registered to **Jacob Green** with email address **greengo8606@gmail.com** (SUBJECT ACCOUNT) for contraband and evidence of violations of Title 18, United States Code, Section 2252A, which is more specifically described in Attachment B of this Affidavit.

4. The statements in this Affidavit are based in part on the information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set for only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence of 18 U.S.C. § 2252A(a)(2)(A)(receipt or distribution of child pornography) and 18 U.S.C. § 2252A(a)(5)(B)(possession of and access with intent to view child pornography) are presently located within the SUBJECT ACCOUNT.

STATUTORY AUTHORITY

5. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to received or distribute, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8) that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

b. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in affecting interstate or foreign commerce, by any means, including by computer, or that was produced in using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

INFORMATION REGARDING KIK MESSENGER

6. Kik messenger (hereinafter, "Kik") is a free instant messaging mobile application designed and previously owned by Kik Interactive Incorporated, a company based in Waterloo, Canada.[1] Kik uses the Internet to allow users to send and receive instant messages, photos and

[1] Kik was purchased in or about October 2019 by MediaLab, Inc., a U.S.-based technology company headquartered in California.

videos. During the account registration process, users are prompted to create a username, which cannot later be changed, and a display or vanity name, which other users initially see when communicating. During the registration process, users are also asked to provide an email address, date of birth, user location, and a profile picture. Email addresses can be "confirmed,' which means the user verified the email address is valid by clicking a link sent from Kik to the provided email address, or "unconfirmed," which means the email address is invalid or the user did not click on the link emailed by Kik. One key feature of Kik is that users are not required to provide accurate information during the account registration process.

7. Once an account is created, a user is able to locate other users through a search feature. The search feature generally requires a user to know an intended recipient's username to locate them. Once connected, Kik users can share messages, images, and videos. Kik also allows users to create chatrooms, through which groups of up to 50 users can exchange messages and digital files. These chatrooms, commonly referred to as "Kik Groups," are administered by the user who created the chatroom, and this user has the authority to add, remove, and ban other users from the group, as well as to promote other users to "administrator." This is true for both private and public chatrooms. Many public groups are created with a group code that contains a "hashtag" (e.g., "#KikTeens"), allowing the group or chatroom to be located more easily.[2] Specifically, a user will search for a public group using a term or word associated with the group name, which is often contained in the hashtag. Once a group is created, Kik users can engage in a "group chat" and exchange messages and content.

[2] The hashtag locating feature is not typically available for private groups.

8. According to Kik's Terms of Service, which each user must acknowledge when creating an account, it is a violation of the agreement to use Kik to upload, post, comment on, or store content that is obscene, offensive, contains child pornography, or is harmful to minors in any way. These Terms of Service specifically state that "…[Kik] may review, screen and delete your User Content at any time if we think it may violate these Terms. You are responsible for the User Content that you send through the Services, including for back up of such content."

9. To combat the proliferation of child pornography on its platform, the Kik Trust and Safety Team uses a third-party company to review pictures that are uploaded by users and groups. Kik also uses PhotoDNA to compare user-uploaded images against a database of known child pornography images that are in circulation. Any images that are flagged and reported by the third-party company or the PhotoDNA software are subsequently viewed by a member of the Kik Trust and Safety Team.

10. Kik also allows users to report other users who have abused or harassed them or others within the application, which include but are not limited to instances of child exploitation and/or child pornography. These are referred to as "Abuse Reports." When a Kik user submits an Abuse Report, they can include their full conversation history, including text and any images or videos transmitted in the conversation. When Kik receives an Abuse Report pertaining to potential or apparent child pornography, an employee reviews the reported material to verify that it contains child pornography or is otherwise considered child exploitative material.

11. Any material determined by Kik to be child pornography or child exploitation through PhotoDNA match, third-party monitoring, or Abuse Reports is subsequently reported to the National Center for Missing and Exploited Children ("NCMEC") via a CyberTipline referral. Kik provides NCMEC with the reported material, as well as basic subscriber information for the

suspect account. This subscriber data includes, but is not limited to, the information entered by the user during the account registration process, any updates to this information after the registration process, device type (e.g., iPbone, Samsung Galaxy S5, etc.), the Kik application version used, and log-in data associated with the last thirty days of account activity. Upon reporting this information to NCMEC, Kik deletes or disables the suspect account for violations its Terms of Service.

12. Based on my training and experience in child exploitation investigations, I am aware that Kik is a prominent meeting place for individuals seeking to share child pornography and engage in child exploitative dialogue. I have investigated several offenders who used Kik to transport, distribute, and receive child pornography, as well as other offenders who used the platform to coerce and entice minors to engage in illegal sexual activity. Based on information obtained from interviews with some of these offenders, I am aware that Kik is a preferred platform for child exploitation offenders because the application facilitates anonymous communication, which assists offenders in avoiding detection by law enforcement.

PROBABLE CAUSE

13. Based on the investigation to date, I believe there is probable cause to believe that a search of the SUBJECT ACCOUNT will discover evidence, fruits, and/or instrumentalities of crimes, including violation of 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt or distribution of child pornography) and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access or attempted to access with intent to view child pornography), and these assets are subject to forfeiture under 18 U.S.C. § 2253.

14. My belief is based upon the following facts and circumstances:

15. The affiant certifies the FBI is conducting a criminal investigation involving the receipt, possession, advertisement, promotion and distribution of child pornography in violation of federal laws, including, but not limited to, Title 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt or distribution of child pornography) and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access or attempted to access with intent to view child pornography), and these assets are subject to forfeiture under 18 U.S.C. § 2253.

16. On April 18, 2023, Kik referred to Operation Rescue Me (ORM), an organization which represents a strategic partnership between FBIHQ and the National Center for Missing and Exploited Children (NCMEC), reported Kik user solidstatewill for uploading two copies of the same video depicting apparent child pornography, which appeared to be produced in the United States. NCMEC evaluates reported material and, when necessary, refers reports of apparent child pornography to the designated law enforcement agency, in this case the FBI. The IP addresses associated with the uploads of these videos by solidstatewill resolve back to Pakistan, and Kik has notified Pakistan of the report made to ORM. The videos appear to be produced by the adult male while he is engaging in sexual intercourse with the adult female. The adult male appears to have a tattoo of black writing on his lower abdomen, but the exact text cannot be determined. The adult female has a black tribal-style tattoo at the small of her back. A prepubescent female and female toddler are also on the bed while the adults are engaging in sexual intercourse. At one point in the video, the female toddler is positioned mostly under the adult female. The prepubescent female is standing on the bed adjacent to the adults engaging in sexual intercourse. Both the prepubescent female and toddler female speak to the adult male, with the female toddler referring to the adult male as "Daddy." The likely created date for the apparent child pornography is September 30, 2021 based on the earliest upload of the video.

17. According to the NCMEC incident report, there were a total of 23 files uploaded from the user "solidstatewill" on the Kik platform, of which two copies of the same video appear to be apparent child pornography. Kik reported user "solidstatewill" concerning apparent child pornography. Files "b13b2dbd-9cca-430a-b413-530b4698ea6d.mp4" and "b13b2dbd-9cca-430a-b413-530b4698ea6d.mp4" appear to depict apparent child pornography. These files were compared with NCMEC's Child Recognition & Identification System (CRIS), and NCMEC had no information on the individuals within these files at the time of the original report. The videos associated with this report were given the NCMEC series name "DotSheet" for tracking purposes and to associate any future images/videos appearing to depict the same individuals. NCMEC performed a "Seen Before Report" on the files associated with this series by running the respective hashes through NCMEC's CRIS, and the hashes have been seen before in CRIS and/or CyberTipline Reports. Video matching technology at NCMEC also returned 29 results of what appear to be additional versions of a visually similar video which have been added to the series. NCMEC was not able to ascertain the identity of the depicted interviewers at that time.

18. FBI Headquarters (FBIHQ) conducted database searches using information in the images and an open source image repository leading to the adults being potentially identified as Jacob and Phila Green of Havelock, NC. FBIHQ determined that Jacob and Phila Green were associated with the address 1 Arthur Drive, Havelock, NC. The following social media accounts were located for Phila and Jacob Green.

Facebook	phila.green
	jacob.green.3133719

19. Photos of children on Phila and Jacob Green's Facebook pages were visually consistent with the two prepubescent females in the apparent child pornography DotSheet series.

20. The Facebook pages of Phila and Jacob Green indicate they have three (3) daughters. The oldest daughter of Phila and Jacob Green is visually consistent to the prepubescent female in the apparent child pornography. The youngest daughter of Phila and Jacob Green is visually consistent with the female toddler in the apparent child pornography. FBIHQ instructed FBI Greenville to conduct an interview of Jacob and Phila Green and conduct any relevant and necessary investigation based on this interview as MCAS Cherry Point falls within FBI Greenville's jurisdiction.

21. FBI Greenville agents (agents) determined that the address associated with Jacob and Phila Green referenced in the original request from FBIHQ, 1 Arthur Drive, Havelock, NC, is located on Marine Corps Air Station (MCAS) Cherry Point. On May 4, 2023, agents liaised with Naval Criminal Investigative Service (NCIS) to determine to confirm that Jacob Green is an active duty Marine and Phila Green is not a member of the military. NCIS further shared that Jacob and Phila Green have three daughters, RG (13), MG (10), and KG (7). Agents confirmed with the Craven County School System (CCSS) that RG and MG were enrolled in Tucker Creek Middle School and Arthur Edwards Elementary School, respectively. CCSS did not have a record of KG's enrollment in any of their schools at that time.

22. On May 8, 2023, agents conducted interviews of Jacob Green, Phila Green, MG and RG. Jacob Green admitted to having created the video referenced in the lead and to creating at least one other video where his children are present. Phila Green admitted to Jacob Green filming videos of the two of them having sexual relations while the children are present either mostly clothed or partially naked. In relation to the video from the FBIHQ lead, Phila Green admitted

that the youngest child, KG, was cupping Phila Green's breasts while Jacob Green was filming the video which was later distributed. Additionally, Phila Green revealed that the Green family takes photographs in which the adults and the children are fully nude which Jacob Green uploads to the nudist website, True Nudist.

23. During the interview with Jacob Green, he disclosed operating the following email and social media accounts:

- Email: Jacob.green@usmc.mil
- Email: vanillasliceusmc@yahoo.com
- Email: Green.machine8606@gmail.com

- Email: greengo8606@gmail.com
- Email: vanillasliceusmc@yahoo.com
- Instagram: Green.machine.8606
- Facebook: Jacob Green
- Snapchat: greengo8613
- Twitter: @gomachine86
- Reddit: Greengo-8606
- Wickr: Unknown
- Tiktok: Greengo86
- Tumblr: Dadbodhero
- Hangouts: unknown
- Skype: Greendotmachine86@hotmail.com
- Kik: Shytxcpl
- Mewe: Jack Bender
- 3rder: Unknown

24. During the interview with Jacob Green, he granted the FBI consent to seize his phone and signed the FD-26 Consent to Search Premises and FD-597 Receipt for property. Jacob Green's phone was submitted to the FBI Computer Analysis Response Team (CART) for data extraction on May 10, 2023.

25. On June 7, 2023, the FBI received subpoena returns for the Kik account provided by Jacob Green (Shytxcpl) and the account which posted the material (solidstatewill_xnw). The

subpoena returns indicate that Shytxcpl is registered to Jacob Green with email greengo8606@gmail.com and that soldistatewill_xnw is registered to William Wontiam with email solidstatewill@gmail.com. Records and database of the name "William Wontiam" did not yield any results.

26. On June 13, 2023, NCMEC provided another cyber tip associated with the DotSheet series for apparent child pornography created by what appears to be the same user, this time reported by Google October 13, 2022. The file was uploaded to Google on September 22, 2022 by user "Sam Tdchb" with associated email address samtdchb@gmail.com. The video appears to also be produced by the adult male from a hand-held device while he is engaging in sexual intercourse with the adult female, both of which appear to match the individuals from the previously-reported video. Three pre-pubescent girls are present in this video, two of which are completely nude and what appears to be the youngest child only in a diaper. The youngest child is holding the adult female's face while the two adults are having intercourse. One of the naked pre-pubescent females is seated on a chair next to the adult male watching the adults have intercourse, and she has her hand on the bare buttocks of the adult female, occasionally spanking the adult female, very close to where the adult male is penetrating the adult female. The three pre-pubescent females in this video match the descriptions and other images of the three Green daughters, and the tattoo on the lower back of the adult female is consistent with the first reported video and a tattoo Phila Green is known to have. The adult male appears to have a black script tattoo on his lower abdomen, the text of which cannot be read.

27. A subpoena to was served to Google LLC on August 8, 2023, and Google LLC did not have any records for email address solidstatewill@gmail.com.

28. While reviewing the ipad Air consensually submitted to the FBI by Phila Green, agents found username Nakedtxcpl associated with email address greengo8606@gmail.com within the email logs saved on the device. An opensource search of the username Nakedtxcpl revealed an account on the nudist website TrueNudist, which depicts the what appears to be the visages of Jacob and Phila Green with listed location set to Havelock, NC. On August 14, 2023, a subpoena was served to SocialCo Media, the parent company for the nudist website TrueNudists for username Nakedtxcpl. The subpoena returns verify that username Nakedtxcpl was registered using email address greengo8606@gmail.com out of Havelock, North Carolina, where the Green family currently resides.

29. On October 18, 2023, a subpoena was served to Google LLC for subscriber information pertaining to Sam Tdchb and email address samtdchb@gmail.com. Google LLC provided returns for the subpoena pertaining to Sam Tdchb on October 18, 2023, and the returns indicate the account was created January 13, 2022; the account was terminated October 11, 2022; and no identification or location information were associated with the account. Database checks did not resolve the name Sam Tdchb or email address samtdchb to a verifiable identity or person.

30. Forensic review of the iphones and tablets consensually seized and searched do not show an apparent link between the accounts or users of soldistatewill_xnw, Sam Tdchb and Shytxcpl, and without the identity of soldistatewill_xnw or Sam Tdchb this connection via these electronic devices is improbable. It is known that Jacob Green filmed apparent child pornography videos with his children present and that at least two other users were in possession of these videos, indicating that these videos were uploaded and/or sent via electronic means. It is known that Kik user solidstatewill posted at least two videos related to the DotSheet series, and it is known that Jacob Green has a registered Kik account under username shytxcpl. The purpose of this warrant

is to uncover the connection between the known possessors of this apparent child pornography, the way in which the apparent child pornography was uploaded and transmitted, other potential recipients or distributors of this series of apparent child pornography and to determine if any other apparent child pornography is maintained on or accessed through this account.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

31. I have had both training and experience in investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers, digital technology and social media and electronic communication accounts are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as digital files that can be directly transferred to a computer by connecting the camera or smartphone to the computer using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone and may be uploaded to social media accounts from several media options.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers and accounts around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic

communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Sometimes individuals interested in children will use multiple different accounts to obtain, view and trade child pornography or to meet and interact with other individuals interested in children or child pornography.

e. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's other accounts, computer, smartphone, or external media in most cases.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ADVERTISE, DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

32. Based on my previous investigative experience related to child sexual exploitation investigations and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals with a sexual interest in children who advertise, distribute, receive, possess, and/or access with intent to view child pornography.

a. Individuals with a sexual interest in children may receive sexual gratification, stimulation, and satisfaction from contact with children or from fantasies they may have viewing

children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs or other visual media, or from literature describing such activity.

b. Individuals with a sexual interest in children may collect sexually explicit or suggestive materials in a variety of accounts and media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibition of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals with a sexual interest in children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including e-mail addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

d. Individuals with a sexual interest in children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if the individual uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found on their social media account, the SUBJECT ACCOUNT, as set forth in Attachment A.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

33. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT ACCOUNT, in whatever form they are found. Thus, the warrant applied for would authorize the seizure of electronically stored storage media or information pertaining to the storage, production or transmission of apparent child pornography, all under Rule 41(e)(2)(B).

34. As further described in Attachment B, this application seeks permission to locate not only media files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the accounts were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the SUBJECT ACCOUNT because:

a. Information stored within a social media account and linked accounts which may provide crucial evidence of the "who, what, when, where, why and who" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within social media account(s) (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, and usage history) can indicate who has used or controlled the account(s). This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. Further, computer and storage media activity can indicate how and when the account(s) was accessed or used. For example, account(s) typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, associated email accounts and phone numbers, payment information, address

information, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of account(s) access, use, and events relating to the crime under investigation. Additionally, some information stored within the account(s) may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images uploaded to the account(s) may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection slogs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the account user. Last, information stored within an account may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the account may indicate the owner's motive and intent to commit a crime (e.g., searches, conversations or affiliations indicating criminal planning), or consciousness of guilt.

All information described above should be shipped to:

Kasey Bratt, Special Agent
Federal Bureau of Investigation
1017 WH Smith Boulevard
Greenville, NC 27834
Cell (571) 456-5716
Or can be emailed to kbratt@fbi.gov

Respectfully Submitted,

Bratt, Kasey, Special Agent
Federal Bureau of Investigation

In accordance with Rule 4.1(b)(2)(A), the Affiant under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, telephone, on this 23 day of February, 2024.

ROBERT B. JONES, JR.
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the **KIK user name shytxcpl** registered to **Jacob Green** with email address **greengo8606@gmail.com** which are stored at premises owned, maintained, controlled, or operated by KIK c/o Media Lab ("Kik"), a company headquartered in Santa Monica, CA.

ATTACHMENT B

Particular Things to be Seized and Procedures

to Facilitate Execution of the Warrant

I. Information to be Disclosed by Kik

To the extent that the information described in Attachment A is within the possession, custody, or control of KIK c/o Media Lab ("Kik"), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs or information that have been deleted but are still available to Kik, or have been preserved pursuant to a request made under 18 U.S.C. SS 2703(f), Kik is required to disclose the following information to the government for each the user account information listed in Attachment A:

(a) All contact and personal identifying information, including **KIK user name shytxcpl** registered to **Jacob Green** with email address **greengo8606@gmail.com**: full names, user identification numbers, birth dates, genders, contact e-mail addresses, Kik passwords, Kik security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Kik activities from August 1, 2020, through the present;

(c) All photos and videos uploaded by that user ID, all photos and videos uploaded by any user that have that user tagged in them, and all photos and videos sent to that user ID from August 1, 2020, through the present, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photographs and videos;

(d) All profile information; friends lists, including the friends Kik user ID numbers; groups and networks of which the user is a member, comments, and information about the user's access and use Kik applications;

(e) All other records of communications and messages made or received by the user from August 1, 2020, through the present, including any messaging activity, private messages, chat history, video calling, streaming, and pending "Friend" requests;

(f) All location-related activity;

(g) All IP logs, including all records of the IP addresses that logged into the account;

(h) All privacy settings and other account settings, including privacy settings for individual Kik posts and activities, and all records showing which Kik users have been blocked or added by the account;

Kik is hereby ordered to disclose the above information to the government within 10 days of service of this warrant.

II. Information to be seized by the government.

All information described above in Section one which constitutes fruits, evidence, or instrumentalities of, or contraband from, violations of 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt or distribution of child pornography) and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access or attempted to access with intent to view child pornography) by the unknown person(s) since at least August 2020 using the subject account identified in Attachment A, information pertaining to the following matters:

(a) Records and evidence pertaining to: the identity of, relationships to, and communications of the suspect(s), any other participant(s), and/or witness(es); the whereabouts of the suspect(s), any co-conspirator(s), and/or other participant(s) on the dates of the offense(s); any steps taken to prepare for and/or to cover-up the offense(s); the methods of the production or distribution of the CSAM.